

PCT/JP2004/005881

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

23. 4. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 3 年 1 2 月 2 6 日

出 願 番 号  
Application Number: 特 願 2 0 0 3 - 4 3 2 4 7 6  
[ST. 10/C]: [ J P 2 0 0 3 - 4 3 2 4 7 6 ]

REC'D 01 JUL 2004

WIPO

PCT

出 願 人  
Applicant(s): 三 菱 電 機 株 式 会 社

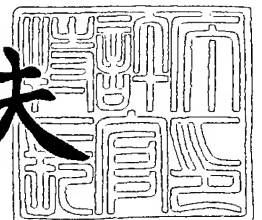
**PRIORITY  
DOCUMENT**

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2 0 0 4 年 6 月 4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 4 8 2 2 5

【書類名】 特許願  
【整理番号】 548699JP01  
【提出日】 平成15年12月26日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 15/00  
【発明者】  
    【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内  
    【氏名】 大越 丈弘  
【発明者】  
    【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内  
    【氏名】 山田 敬喜  
【発明者】  
    【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内  
    【氏名】 牧田 覚  
【特許出願人】  
    【識別番号】 000006013  
    【氏名又は名称】 三菱電機株式会社  
【代理人】  
    【識別番号】 100099461  
    【弁理士】  
    【氏名又は名称】 溝井 章司  
【手数料の表示】  
    【予納台帳番号】 056177  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1

**【書類名】 特許請求の範囲****【請求項 1】**

少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶する記憶部と、

上記記憶部により記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを認証装置に送信する送信部と、

上記認証装置から上記送信部により送信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部と、

上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子に基づいて上記認証装置との間で認証処理をおこなう認証処理部とを備えたことを特徴とする被認証装置。

**【請求項 2】**

上記記憶部は、1 つのアルゴリズム識別子と 1 つの暗号鍵識別子とを 1 組のプロファイルとして、少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶し、

上記送信部は、上記記憶部により 1 つのアルゴリズム識別子と 1 つの暗号鍵識別子とを 1 組のプロファイルとして記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを認証装置に送信し、

上記受信部は、上記認証装置から上記送信部により送信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中から所定のプロファイルとして組となる上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とを受信し、

上記認証処理部は、上記受信部により受信された所定のプロファイルとして組となる所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする請求項 1 記載の被認証装置。

**【請求項 3】**

上記記憶部は、さらに、記憶された少なくとも 1 つのアルゴリズム識別子に対応する少なくとも 1 つのアルゴリズムを 1 つのセットとした上記セットを示すバージョンを識別するバージョン識別子を記憶し、

上記送信部は、上記記憶部により記憶されたバージョン識別子を認証装置に送信し、

上記受信部は、上記認証装置から上記送信部により送信されたバージョン識別子が識別するバージョンが示すセットとなる少なくとも 1 つのアルゴリズムの中の所定のアルゴリズムに対応する上記所定のアルゴリズム識別子を受信し、

上記認証処理部は、上記受信部により受信された所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記認証装置との間で認証処理をおこなうことを特徴とする請求項 2 記載の被認証装置。

**【請求項 4】**

少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶する記憶部と、

被認証装置から少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを受信する受信部と、

上記受信部により受信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中に上記記憶部により記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とが存在する場合に、上記受信部により受信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中から上記記憶部により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択部と、

上記選択部により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記被認証装置に送信する送信部と、

上記送信部により送信される所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づ

いて上記被認証装置との間で認証処理をおこなう認証処理部とを備えたことを特徴とする認証装置。

【請求項 5】

上記記憶部は、少なくとも 1つのアルゴリズム識別子の 1つのアルゴリズム識別子と少なくとも 1つの暗号鍵識別子の 1つの暗号鍵識別子とを組とする少なくとも 1つのプロファイルを識別する少なくとも 1つのプロファイル識別子を記憶し、

上記受信部は、さらに、上記被認証装置から少なくとも 1つのプロファイル識別子を受信し、

上記選択部は、上記受信部により受信された少なくとも 1つのプロファイル識別子の中に上記記憶部により記憶された少なくとも 1つのプロファイル識別子が存在する場合に、上記受信部により受信された少なくとも 1つのプロファイル識別子の中から上記記憶部により記憶される所定のプロファイル識別子を選択し、

上記送信部は、上記選択部により選択された所定のプロファイル識別子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のプロファイル識別子により識別される所定のプロファイルが組とする上記所定のアルゴリズム識別子と上記所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする請求項 4 記載の認証装置。

【請求項 6】

上記記憶部は、さらに、記憶された少なくとも 1つのアルゴリズム識別子に対応する少なくとも 1つのアルゴリズムを 1つのセットとして、上記セットのバージョンを識別するバージョン識別子を記憶し、

上記受信部は、さらに、上記被認証装置から所定のバージョン識別子を受信し、

上記選択部は、上記受信部により受信された所定のバージョン識別子が識別するバージョンが示すセットの中の 1つのアルゴリズムに対応する上記所定のアルゴリズム識別子を選択し、

上記送信部は、上記選択部により選択された所定のアルゴリズム識別子を上記被認証装置に送信し、

上記認証処理部は、上記送信部により送信される所定のアルゴリズム識別子と上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子とに基づいて上記被認証装置との間で認証処理をおこなうことを特徴とする請求項 5 記載の認証装置。

【請求項 7】

複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信する第 1 の送信工程と、

少なくとも 1つのアルゴリズム識別子と少なくとも 1つの暗号鍵識別子とを記憶する認証装置が、上記第 1 の送信工程により被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信する第 1 の受信工程と、

上記第 1 の受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも 1つのアルゴリズム識別子と少なくとも 1つの暗号鍵識別子とが存在する場合に、上記認証装置が上記受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第 2 の送信工程と、

上記被認証装置が上記認証装置から上記第 2 の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第 2 の受信工程と、

上記第 2 の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えたことを特徴とする認証方法。

**【請求項 8】**

少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを認証装置に送信する第 1 の送信工程と、

複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装置が、上記第 1 の送信工程により被認証装置から送信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを受信する第 1 の受信工程と、

上記第 1 の受信工程により受信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム識別子の少なくとも 1 つと複数の暗号鍵識別子の少なくとも 1 つとが存在する場合に、上記認証装置が上記受信工程により受信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、

上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第 2 の送信工程と、

上記被認証装置が上記認証装置から上記第 2 の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第 2 の受信工程と、

上記第 2 の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えたことを特徴とする認証方法。

【書類名】明細書

【発明の名称】被認証装置及び認証装置及び認証方法

【技術分野】

【0001】

本発明は、被認証装置、或いは認証装置に関する。または、上記認証装置と上記被認証装置との間で認証をおこなう認証方法に関する。

【背景技術】

【0002】

利用者があるサービスを受けるとき、サービスを受けられる正当な利用者であるかどうか本人確認（認証）が行なわれ、暗号通信のための鍵共有が行なわれる。暗号通信に用いられる暗号アルゴリズムは1種類であり、異なるアルゴリズムを実装している装置間では認証及び鍵共有が行えない。

【0003】

また、複数の暗号技術利用プロトコルの利用が可能な通信システムについての記載が載った文献が存在する（特許文献1参照）。

【0004】

また、複数のアルゴリズムを用いた技術についての記載が載った文献が存在する（特許文献2，3参照）。

【特許文献1】特開平10-304333号公報

【特許文献2】特開2000-151578号公報

【特許文献3】特開平5-227152号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

以上のように、従来は、暗号通信に用いられる暗号アルゴリズムは1種類であるため、アルゴリズムの脆弱性が発見されたり、解読されたり、鍵の漏洩等によりデータ暗号化によるセキュリティ（安全）が保たれなくなった場合に、より安全なアルゴリズム等を実装することになるが、これにより装置間で異なるアルゴリズムを実装する場合が生じ、上述したように異なるアルゴリズムを実装している装置間では認証及び鍵共有が行えないといった問題があった。また、各メーカー等がそれぞれ販売等している暗号アルゴリズムがあるために、異なるアルゴリズムを実装している装置間では認証及び鍵共有が行えないといった問題があった。

【0006】

また、上述したようにセキュリティ（安全）が保たれなくなった場合に、より安全なアルゴリズムを実装することになるが、新たなアルゴリズム等を実装することによりそれまでのシステム及び装置が使い物にならなくなるといった問題があった。

【0007】

また、将来、より高度なアルゴリズムが考案されたとしてもそれまで使用していた装置に適用することができないといった問題があった。

【0008】

本発明は、搭載しているアルゴリズムが異なるために認証が行えないといった問題を解決することを目的とする。

【0009】

本発明は、1つのアルゴリズムが解読等により使用できなくなっても引き続きシステム及び装置を運用可能とすることを目的とする。

【0010】

また、本発明は、引き続きシステム及び装置を運用可能とすることで、アルゴリズムの解読等によるセキュリティ低下というリスクを軽減することを目的とする。

【0011】

また、本発明は、盗聴等による不正な解読等の機会を減らし、セキュリティを向上させ

ることを目的とする。

【課題を解決するための手段】

【0012】

この発明に係る被認証装置は、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する記憶部と、

上記記憶部により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信する送信部と、

上記認証装置から上記送信部により送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部と、

上記受信部により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子に基づいて上記認証装置との間で認証処理をおこなう認証処理部とを備えたことを特徴とする。

【発明の効果】

【0013】

本発明によれば、異なるアルゴリズムを実装している装置間でも認証及び鍵共有が行なえるようにすることができ、1つのアルゴリズムが解読等により使用できなくなっても引き続きシステム及び装置を運用可能とすることができる。

【0014】

また、アルゴリズムの解読等によるセキュリティ低下というリスクを軽減することができる。

【0015】

また、盗聴等による不正な解読等の機会を減らし、セキュリティを向上させることができる。

【発明を実施するための最良の形態】

【0016】

実施の形態1.

図1は、実施の形態1における認証システムの構成を示す図である。

【0017】

図1において、認証システムは、認証装置となる通信装置100と被認証装置となる通信装置200とを備えている。通信装置100は、アンテナ101、通信処理部110、記憶部120、制御部130、選択部160、認証処理部196を備えている。通信処理部110は、受信部111、送信部112を有している。認証処理部196は、暗号処理部140、乱数生成部150、個別鍵生成部170、一時鍵生成部180、認証用データ1生成部190、認証用データ2チェック部195を有している。通信装置200は、アンテナ201、通信処理部210、記憶部220、制御部230、認証処理部296を備えている。通信処理部210は、受信部211、送信部212を有している。認証処理部296は、暗号処理部240、乱数生成部250、一時鍵生成部280、認証用データ1チェック部290、認証用データ2生成部295を有している。実施の形態1では、通信装置100と通信装置200とは、アンテナ101、201を介して無線通信する場合を説明するが、これに限るものではなく有線通信であっても構わない。例えば、ETC（料金自動収集）、ドライブスルー等において、通信装置100は、店舗側の路側機として、通信装置200は、自動車側の車載機として構成される。

【0018】

図2は、実施の形態1における認証方法を示すフローチャート図である。

【0019】

記憶部120は、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子と、上記少なくとも1つのアルゴリズム識別子の各アルゴリズム識別子に対応するアルゴリズムを記憶している。また、上記記憶部120は、少なくとも1つのアルゴリズム識別子の1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子の1つの暗号鍵識別子

とを組とする少なくとも1つのプロファイルを識別する少なくとも1つのプロファイル識別子を記憶している。

#### 【0020】

記憶部220は、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子と、上記少なくとも1つのアルゴリズム識別子の各アルゴリズム識別子に対応するアルゴリズムと上記少なくとも1つの暗号鍵識別子の各暗号鍵識別子に対応する暗号鍵となる装置固有の個別鍵と装置固有番号とを記憶している。また、上記記憶部220は、1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とプロファイルを識別する少なくとも1つのプロファイル識別子とを記憶している。

#### 【0021】

ここで、通信装置100、200のうち、少なくとも一方において、アルゴリズム識別子と暗号鍵識別子との組が複数存在すればよい。

#### 【0022】

S(ステップ)201において、認証処理工程の一部として、乱数生成部150は、乱数1を生成する。

#### 【0023】

S202において、送信工程として、送信部112は、乱数生成部150により生成された乱数1を通信情報1として通信装置200に送信する。例えば、通信装置200を搭載した自動車が、通信装置100により図示していない検知器により検知された場合に、送信部112は、乱数1を通信装置200に送信する。通信装置100は、乱数1を通信情報1として通信装置200に送信することで、通信装置200が保持している鍵情報(鍵識別子、アルゴリズム識別子)を要求する。言い換えれば、通信情報1が通信装置200への要求情報となる。

#### 【0024】

S203において、受信工程として、受信部211は、送信部112により送信された乱数1を通信情報1として受信する。通信装置200では、受信部211が、乱数1を受信したことにより、通信装置100より通信装置200が保持している鍵情報(鍵識別子、アルゴリズム識別子)が要求されたと判断する。

#### 【0025】

S204において、認証処理工程の一部として、乱数生成部250は、乱数2を生成する。

#### 【0026】

S205において、送信工程(第1の送信工程)として、送信部212は、上記記憶部220により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子と装置固有番号と、乱数生成部250により生成された乱数2とを通信情報2として認証装置である通信装置200に送信する。ここで、1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組みとしてプロファイルとして表し、通信情報2は、乱数2と装置固有番号と組数分のプロファイル数とプロファイル数分の各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とをデータとして有している。さらに、ここでは、各プロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子とを対応させたデータとしている。言い換えれば、上記送信部212は、上記記憶部220により1つのアルゴリズム識別子と1つの暗号鍵識別子とを1組のプロファイルとして記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置となる通信装置100に送信する。

#### 【0027】

S206において、受信工程(第1の受信工程)として、受信部111は、被認証装置となる通信装置200から、乱数2と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも1つのプロファイル識別子と少なくとも1つのプロファイル識別子



の各プロファイル識別子に対応した少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを有する通信情報2を受信する。

#### 【0028】

S207において、選択工程として、選択部160は、上記受信部111により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中に上記記憶部120により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とが存在する場合に、上記受信部111により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から上記記憶部120により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する。言い換えれば、上記選択部160は、上記受信部111により受信された少なくとも1つのプロファイル識別子の中に上記記憶部120により記憶された少なくとも1つのプロファイル識別子が存在する場合に、上記受信部111により受信された少なくとも1つのプロファイル識別子の中から上記記憶部120により記憶される所定のプロファイル識別子を選択する。所定のプロファイル識別子を選択することで、所定のプロファイル識別子が示すプロファイルに組みする所定のアルゴリズム識別子と所定の暗号鍵識別子とが選択される。例えば、単純に、通信装置100、200双方が共通して有しているアルゴリズム識別子と暗号鍵識別子とを選択してもよいし、暗号解読等により既にセキュリティが十分でなくなったアルゴリズム識別子と暗号鍵識別子とを排除した上で、通信装置100、200双方が共通して有しているアルゴリズム識別子と暗号鍵識別子とを選択してもよい。また、実施の形態1では、所定のプロファイル識別子を選択することで、所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とを選択する。

#### 【0029】

S208において、認証処理工程の一部として、個別鍵生成部170は、上記選択部160により選択された所定の暗号鍵識別子に対応する暗号鍵となる通信装置200が有している個別鍵を通信情報2の装置固有番号から例えばハッシュ値等を用いて生成する。

#### 【0030】

S209において、認証処理工程の一部として、一時鍵生成部180は、上記選択部160により選択された所定のアルゴリズム識別子に対応するアルゴリズムを用いて所定の暗号鍵識別子に対応する暗号鍵となる個別鍵生成部170により生成された個別鍵で乱数1、2を暗号処理部140を用いて暗号化し、認証処理用暗号鍵の一例となる一時鍵を生成する。

#### 【0031】

S210において、認証処理工程の一部として、認証用データ1生成部190は、乱数2のすべて或いは一部を暗号処理部140により一時鍵生成部180により生成された一時鍵で暗号化することにより認証用データ1を生成する。

#### 【0032】

S211において、送信工程（第2の送信工程）として、送信部112は、上記選択部160により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と上記選択部により選択された対応する所定のプロファイル識別子と認証用データ1生成部190により生成された認証用データ1とを通信情報3として上記被認証装置となる通信装置200に送信する。

#### 【0033】

S212において、受信部211は、上記認証装置となる通信装置100から上記送信部212により送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子と所定のアルゴリズム識別子と所定の暗号鍵識別子と対応するプロファイル識別子と認証用データ1とを通信情報3として受信する。言い換えれば、上記受信部211は、上記認証装置となる通信装置100から上記送信部212により送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から所定のプロファイルとして組となる所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する。

**【0034】**

S213において、認証処理工程の一部として、暗号処理部240は、受信部211により受信されたプロファイル識別子を確認し、プロファイル識別子に対応する所定の暗号鍵識別子と所定のアルゴリズム識別子とを確認する。

**【0035】**

S214において、認証処理工程の一部として、一時鍵生成部280は、受信部211により受信され、暗号処理部240により確認された所定のアルゴリズム識別子に対応するアルゴリズムを用いて、記憶部220に記憶された個別鍵で乱数1, 2を暗号処理部240を用いて暗号化し、認証処理用暗号鍵の一例となる上記一時鍵を生成する。以上により通信装置100, 200間で同じ一時鍵という鍵共有ができたことになる。なお、記憶部220に記憶された個別鍵は、個別鍵生成部170と同様の生成方法で生成されたものであり、あらかじめ、ICカード等何かしらの手段を用いて記憶部220に記録されている。なお、この実施形態では、一時鍵生成部180, 280が一時鍵生成の際、個別鍵で暗号化したが、認証装置と被認証装置とが同じ処理を実施すればよいため、復号してもよい。

**【0036】**

S215において、認証処理工程の一部として、認証用データ1チェック部290は、受信部211により通信情報3として受信された暗号化されている認証用データ1を一時鍵生成部280により生成された一時鍵により暗号処理部240を用いて復号する。

**【0037】**

S216において、認証処理工程の一部として、認証用データ1チェック部290は、復号した認証用データ1のデータが、通信装置200が通信装置100に送信した乱数2のすべて或いは一部であるかどうかを確認する。復号した認証用データ1のデータが乱数2のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置100との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置100, 200間での認証処理の一方が成功したことを意味する。

**【0038】**

S217において、認証処理工程の一部として、認証用データ2生成部295は、乱数1のすべて或いは一部を暗号処理部240により一時鍵生成部280により生成された一時鍵で暗号化することにより認証用データ2を生成する。

**【0039】**

S218において、認証処理工程の一部の送信工程として、送信部212は、認証用データ2生成部295により生成された認証用データ2を通信情報4として通信装置100に送信する。

**【0040】**

S219において、認証処理工程の一部の受信工程として、受信部111は、通信装置200から認証用データ2を通信情報4として受信する。

**【0041】**

S220において、認証処理工程の一部として、認証用データ2チェック部195は、受信部111により通信情報4として受信された暗号化されている認証用データ2を一時鍵生成部180により生成された一時鍵により暗号処理部140を用いて復号する。

**【0042】**

S221において、認証処理工程の一部として、認証用データ2チェック部195は、復号した認証用データ2のデータが、通信装置100が通信装置200に送信した乱数1のすべて或いは一部であるかどうかを確認する。復号した認証用データ2のデータが乱数1のすべて或いは一部であれば、不正の攻撃者との間ではなく、通信装置200との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置100, 200間での認証処理の他方が成功したことを意味する。

**【0043】**

以上により、通信装置100, 200間での認証処理が終了し、その後は、通信装置1

0 0 , 2 0 0 間で一時鍵を用いて暗号化されたデータを通信することにより、データの安全性が確保される。

【 0 0 4 4 】

図 3 は、通信情報 1 のフレームの一例を示す図である。

【 0 0 4 5 】

図 3 において、通信情報 1 は、ヘッダと乱数 1 データを有している。

【 0 0 4 6 】

図 4 は、通信情報 2 のフレームの一例を示す図である。

【 0 0 4 7 】

図 4 において、通信情報 2 は、ヘッダと乱数 2 データと装置固有番号（装置固有 No.）とプロファイル数（Profile 数）と各プロファイルを識別するプロファイル識別子としての Profile 1, . . . Profile n と、各プロファイル識別子に対応するアルゴリズム識別子（アルゴリズム ID）と暗号鍵識別子（鍵 ID）とを有している。図 4 では、各プロファイル識別子と各プロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

【 0 0 4 8 】

図 5 は、通信情報 3 のフレームの一例を示す図である。

【 0 0 4 9 】

図 5 において、通信情報 3 は、ヘッダと選択された所定のプロファイルを識別する所定のプロファイル識別子としての Profile k と、所定のプロファイル識別子に対応するアルゴリズム識別子（アルゴリズム ID）と暗号鍵識別子（鍵 ID）と認証用データ 1 とを有している。図 5 では、所定のプロファイル識別子と所定のプロファイル識別子に対応するアルゴリズム識別子と暗号鍵識別子とは、対応関係がわかるようにデータが構成されている。

【 0 0 5 0 】

図 6 は、通信情報 4 のフレームの一例を示す図である。

【 0 0 5 1 】

図 6 において、通信情報 4 は、ヘッダと認証用データ 2 とを有している。

【 0 0 5 2 】

図 7 は、通信装置 2 0 0 側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムと個別鍵とを示す図である。

【 0 0 5 3 】

図 7 において、通信装置 2 0 0 側では、記憶部 2 2 0 に、プロファイル x x のアルゴリズム識別子（ID）と暗号鍵識別子（ID）とアルゴリズム識別子に対応するアルゴリズム x と暗号鍵識別子に対応する個別鍵 x と、プロファイル y y のアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム y と暗号鍵識別子に対応する個別鍵 y と、. . . プロファイル z z のアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム z と暗号鍵識別子に対応する個別鍵 z とが記憶されている。すなわち、通信装置 2 0 0 に搭載（実装）されている。

【 0 0 5 4 】

図 8 は、通信装置 1 0 0 側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムとを示す図である。

【 0 0 5 5 】

図 8 において、通信装置 1 0 0 側では、記憶部 1 2 0 に、プロファイル a a のアルゴリズム識別子（ID）と暗号鍵識別子（ID）とアルゴリズム識別子に対応するアルゴリズム 1 と、プロファイル b b のアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム 2 と、. . . プロファイル c c のアルゴリズム識別子と暗号鍵識別子とアルゴリズム識別子に対応するアルゴリズム n とが記憶されている。すなわち、通信装置 1 0 0 に搭載（実装）されている。

【 0 0 5 6 】

以上のように、認証処理部 2 9 6 は、上記受信部 2 1 1 により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置となる通信装置 1 0 0 との間で認証処理をおこなう。すなわち、認証処理部 2 9 6 は、上記受信部 2 1 1 により受信された所定のアルゴリズム識別子に対応するアルゴリズムと上記受信部により受信された所定の暗号鍵識別子に対応する暗号鍵とを用いて認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記認証装置となる通信装置 1 0 0 との間で認証処理をおこなう。言い換えれば、上記認証処理部 2 9 6 は、上記受信部 2 1 1 により受信された所定のプロファイルとして組となる所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記認証装置との間で認証処理をおこなう。

#### 【 0 0 5 7 】

一方、認証処理部 1 9 6 は、上記送信部 1 1 2 により送信される所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記被認証装置となる通信装置 2 0 0 との間で認証処理をおこなう。すなわち、認証処理部 1 9 6 は、上記送信部 1 1 2 により送信される所定のアルゴリズム識別子に対応するアルゴリズムと上記送信部 1 1 2 により送信された所定の暗号鍵識別子に対応する暗号鍵とを用いて認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記被認証装置となる通信装置 2 0 0 との間で認証処理をおこなう。言い換えれば、上記認証処理部 1 9 6 は、上記送信部 1 1 2 により送信される所定のプロファイル識別子により識別される所定のプロファイルが組とする所定のアルゴリズム識別子に対応するアルゴリズムと所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵となる一時鍵を生成し、生成された認証処理用暗号鍵となる一時鍵を用いて上記被認証装置との間で認証処理をおこなう。

#### 【 0 0 5 8 】

ここで、制御部 1 3 0 は、通信装置 1 0 0 の各部を制御する。また、制御部 2 3 0 は、通信装置 2 0 0 の各部を制御する。また、記憶部 1 2 0 は、通信装置 1 0 0 の各部で行なわれる処理中に生じるデータを記憶する。また、記憶部 2 2 0 は、通信装置 2 0 0 の各部で行なわれる処理中に生じるデータを記憶する。

#### 【 0 0 5 9 】

例えば、一例として、E T C、ドライブスルー等において、通信装置 1 0 0 が、店舗側の路側機として、通信装置 2 0 0 が、自動車側の車載機として構成される場合に、以上のステップを概括すると以下ようになる。

#### 【 0 0 6 0 】

まず、店舗側の路側機は、車載機に対して、車載機が保持している鍵情報（鍵識別子、アルゴリズム識別子）を要求する。

#### 【 0 0 6 1 】

そして、車載機は、自身が保持している鍵に関する全情報を路側機に送信する。

#### 【 0 0 6 2 】

次に、路側機は、受け取った鍵情報の中から、自身が保持しているアルゴリズム識別子と鍵識別子とが一致しているものを選択し、車載機に選択したアルゴリズム識別子と鍵識別子とを知らせる。

#### 【 0 0 6 3 】

以降、路側機及び車載機は、お互いに共通に保持していたアルゴリズム識別子と鍵識別子とに対応する共通鍵を用いて認証及び鍵共有を実施する。

#### 【 0 0 6 4 】

以上のように、本実施の形態 1 は、暗号通信に用いるアルゴリズムを複数に対応させるもので、1つのアルゴリズムが解読等で使用できなくなっても他のアルゴリズムを使用することで、引き続きシステムを運用可能とし、アルゴリズム解読等によるセキュリティ低下というリスクを軽減させることができる。また、複数のアルゴリズムを使いこなすことにより、同一のアルゴリズムを使用する回数が減ることにより、不正の攻撃者による解読

の機会を減らし、セキュリティを向上させることができる。さらに、新たに考案されたアルゴリズムを通信装置に搭載することができることから、新たに考案されたアルゴリズムの適用をも容易にすることができる。通信装置 100, 200 のうち、少なくとも一方において、アルゴリズム識別子と鍵識別子との組が複数存在すれば、選択肢ができることになり、上記効果が得られる。なお、この実施形態 1 では、装置 100, 200 の少なくとも一方に複数のアルゴリズム識別子と暗号鍵識別子との組が複数存在すればよいとした。しかし、この発明はアルゴリズム識別子と暗号鍵識別子の少なくとも 1 組が一致すれば認証が行えるため、必ずしも装置 100, 200 の少なくとも一方に複数組存在する必要はなく各装置に 1 組だけが存在していてもよい。また、各装置に 1 組だけしか存在していてもよいことから、一つの暗号アルゴリズムしか使用しない従来例にもこの発明による認証方法を適用可能である。

#### 【0065】

実施の形態 2.

図 9 は、実施の形態 2 における認証システムの構成を示す図である。

#### 【0066】

図 9 において、通信装置 200 における認証処理部 296 は、図 1 の構成に対し、さらに、認証用データ 1 生成部 291 を有している。その他の各構成は、図 1 と同様である。

#### 【0067】

図 10 は、実施の形態 2 における認証方法を示すフローチャート図である。

#### 【0068】

図 10 において、図 2 の S215, S216 が S1015, S1016 に代わった以外は、図 2 と同様である。

#### 【0069】

S1015 において、認証処理工程の一部として、認証用データ 1 生成部 291 は、乱数 2 のすべて或いは一部を暗号処理部 240 により一時鍵生成部 280 により生成された一時鍵で暗号化することにより認証用データ 1 を生成する。

#### 【0070】

S1016 において、認証処理工程の一部として、認証用データ 1 チェック部 290 は、通信情報 3 として受信部 211 により受信された暗号化されたままの認証用データ 1 と認証用データ 1 生成部 291 により生成された認証用データ 1 とが一致するかどうかを確認する。一致すれば、不正の攻撃者との間ではなく、通信装置 100 との間で認証処理のための通信がきちっと行なわれていることを意味する。言い換えれば、通信装置 100, 200 間での認証処理の一方が成功したことを意味する。

#### 【0071】

以上のように構成しても実施の形態 1 と同様の効果を得ることができる。

#### 【0072】

実施の形態 3.

実施の形態 3 における各構成は、図 1 と同様である。

#### 【0073】

図 11 は、実施の形態 3 における認証方法を示すフローチャート図である。

#### 【0074】

図 11 では、図 2 の S202, S203 が無いこと以外は、図 2 と同様である。

#### 【0075】

実施の形態 3 では、認証側となる通信装置 100 が通信装置 200 に通信情報 1 を送信しなくても通信装置 200 から通信装置 100 へ通信情報 2 を送信する構成となっている。かかるステップを省略することにより、より高速に認証フローを実施することができる。

#### 【0076】

以上のように構成しても実施の形態 1 と同様の効果を得ることができる。

#### 【0077】

実施の形態 4.

実施の形態 4 における各構成は、図 1 と同様である。

【0078】

図 12 は、実施の形態 4 における認証方法を示すフローチャート図である。

【0079】

図 12 では、図 2 の S205、S206、S207、S211、S212 が、S1205、S1206、S1207、S1211、S1212 に代わった以外は、図 2 と同様である。

【0080】

実施の形態 4 では、記憶部 220 は、さらに、記憶された少なくとも 1 つのアルゴリズム識別子に対応する少なくとも 1 つのアルゴリズムを 1 つのセットとした上記セットを示すバージョンを識別するバージョン識別子 (ID) を記憶する。

【0081】

同様に、記憶部 120 は、さらに、記憶された少なくとも 1 つのアルゴリズム識別子に対応する少なくとも 1 つのアルゴリズムを 1 つのセットとして、上記セットのバージョンを識別するバージョン識別子 (ID) を記憶する。

【0082】

例えば、バージョン識別子としてのバージョン 1 が識別するバージョンは、アルゴリズムとして DES だけをサポートする。バージョン 2 が識別するバージョンは、アルゴリズムとして DES、MISTY をサポートする。バージョン 3 が識別するバージョンは、アルゴリズムとして DES、MISTY、Camellia、AES をサポートする。

【0083】

S1205 において、送信工程 (第 1 の送信工程) として、送信部 212 は、上記記憶部 220 により記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子と装置固有番号と、乱数生成部 250 により生成された乱数 2 と、さらに、記憶部 220 により記憶されたバージョン識別子とを通信情報 2-1 として認証装置である通信装置 100 に送信する。

【0084】

S1206 において、受信工程 (第 1 の受信工程) として、受信部 111 は、被認証装置となる通信装置 200 から、乱数 2 と装置固有番号と組数分のプロファイル数とプロファイル数分の少なくとも 1 つのプロファイル識別子と少なくとも 1 つのプロファイル識別子の各プロファイル識別子に対応した少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子と、さらに、所定のバージョン識別子とを有する通信情報 2-1 を受信する。

【0085】

S1207 において、選択工程として、選択部 160 は、上記受信部 111 により受信された所定のバージョン識別子が識別するバージョンが示すセットの中に上記記憶部 120 により記憶された少なくとも 1 つのアルゴリズムが存在する場合に、上記受信部 111 により受信された所定のバージョン識別子が識別するバージョンが示すセットの中から上記記憶部 120 により記憶されるアルゴリズムに対応する所定のアルゴリズム識別子を選択する。例えば、通信装置 200 が古いバージョンしか対応していない場合に、古いバージョンが示すアルゴリズムがすべてセキュリティ上問題がある場合、選択せずに以降の認証処理を終了させることもできる。一方、1 つでも認証処理に使用可能なアルゴリズムがあれば、その使用可能なアルゴリズムを使って、以降の認証処理を行なわせることができる。バージョン識別子を用いることで、バージョン識別子から通信装置 200 が使用可能なアルゴリズムを搭載しているかどうかを判断することができる。

【0086】

S1211 において、送信工程 (第 2 の送信工程) として、送信部 112 は、上記選択部 160 により選択された所定のアルゴリズム識別子と認証用データ 1 生成部 190 により生成された認証用データ 1 とを通信情報 3-1 として上記被認証装置となる通信装置 2

00に送信する。

【0087】

S1212において、受信工程として、受信部211は、上記認証装置となる通信装置100から上記送信部212により送信されたバージョン識別子が識別するバージョンが示すセットとなる上記記憶部220により記憶された少なくとも1つのアルゴリズムの中から選択された所定のアルゴリズムに対応する所定のアルゴリズム識別子と認証用データ1とを通信情報3-1として受信する。

【0088】

以降、認証処理部296は、上記受信部211により受信された所定のアルゴリズム識別子に対応する所定のアルゴリズムと上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子に対応する所定の暗号鍵とを用いて上記認証処理用暗号鍵を生成し、生成された認証処理用暗号鍵を用いて上記認証装置との間で認証処理をおこなう。

【0089】

同様に、認証処理部196は、上記送信部112により送信される所定のアルゴリズム識別子に対応するアルゴリズムと上記所定のアルゴリズム識別子と組となる所定の暗号鍵識別子に対応する暗号鍵とを用いて上記認証処理用暗号鍵を生成し、生成された認証処理用暗号鍵を用いて上記被認証装置との間で認証処理をおこなう。

【0090】

以上のように構成することで、実施の形態1の効果に加え、セキュリティ上問題がある古いバージョンを排除することもできる。

【0091】

ここで、実施の形態4では、選択部160が、所定のアルゴリズム識別子を選択しているが、さらに、選択した所定のアルゴリズム識別子に対応する所定の暗号鍵識別子を選択してもかまわない。かかる場合、図12におけるS1211、S1212は、図2におけるS211、S212のままで構わない。

【0092】

実施の形態5.

実施の形態5における各構成は、図1と同様である。

【0093】

図13は、実施の形態5における認証方法を示すフローチャート図である。

【0094】

図13では、図2のS205、S206、S207が、S1305、S1306、S1307、S1308、S1309、S1310、S1311、S1307に代わった以外は、図2と同様である。

【0095】

実施の形態5では、実施の形態4と同様に、記憶部220は、さらに、記憶された少なくとも1つのアルゴリズム識別子に対応する少なくとも1つのアルゴリズムを1つのセットとした上記セットを示すバージョンを識別するバージョン識別子(ID)を記憶する。

【0096】

同様に、記憶部120は、さらに、記憶された少なくとも1つのアルゴリズム識別子に対応する少なくとも1つのアルゴリズムを1つのセットとして、上記セットのバージョンを識別するバージョン識別子(ID)を記憶する。

【0097】

S1305において、送信工程として、送信部212は、上記記憶部220により記憶された装置固有番号と、乱数生成部250により生成された乱数2と、さらに、記憶部220により記憶されたバージョン識別子とを通信情報2-2として認証装置である通信装置200に送信する。

【0098】

S1306において、受信工程（第1の受信工程）として、受信部111は、被認証装置となる通信装置200から、乱数2と装置固有番号と所定のバージョン識別子とを有す



る通信情報 2-2 を受信する。

【0099】

S1307において、選択工程として、選択部160は、上記受信部111により受信された所定のバージョン識別子が、記憶部120に記憶されたバージョン識別子と一致する場合は、そのバージョン識別子を選択し、一致しない場合には、所定のバージョン識別子が示すセットの中に上記記憶部120により記憶された少なくとも1つのアルゴリズムが存在する場合に、上記記憶部120により記憶された少なくとも1つのアルゴリズムが存在するセットを示すバージョンのバージョン識別子を選択する。例えば、記憶部120に記憶されたバージョン識別子の方が、上記受信部111により受信された所定のバージョン識別子より最新バージョンのバージョン識別子である場合に、通信装置100、200に共通するように古いバージョンとなる上記受信部111により受信された所定のバージョン識別子を選択する。通信装置100、200に共通する古いバージョンを選択することにより以降の認証処理を続行させ、鍵共有をおこなうことができる。

【0100】

S1308において、送信工程として、送信部112は、選択部160により選択されたバージョン識別子(ID)を通信情報2-3として通信装置200に送信する。

【0101】

S1309において、受信工程として、受信部211は、通信装置100よりバージョン識別子(ID)を通信情報2-3として受信する。

【0102】

S1310において、送信工程として、送信部212は、上記記憶部220により記憶された少なくとも1つのプロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子と組数分のプロファイル数とを通信情報2-4として認証装置である通信装置200に送信する。

【0103】

S1311において、受信工程として、受信部111は、被認証装置となる通信装置200から、少なくとも1つのプロファイル識別子と各プロファイル識別子が表すプロファイルに組とされるアルゴリズム識別子と暗号鍵識別子と組数分のプロファイル数とを通信情報2-4として受信する。ここで、乱数2と装置固有番号とを通信情報2-2に含めているが、通信情報2-4に含めていても構わない。

【0104】

S1312において、選択工程として、選択部160は、上記受信部111により受信された少なくとも1つのプロファイル識別子の中に上記記憶部120により記憶された少なくとも1つのプロファイル識別子が存在する場合に、上記受信部111により受信された少なくとも1つのプロファイル識別子の中から上記記憶部120により記憶される所定のプロファイル識別子を選択する。所定のプロファイル識別子を選択することで、所定のプロファイル識別子が示すプロファイルに組みする所定のアルゴリズム識別子と所定の暗号鍵識別子とが選択される。

【0105】

以上のように、実施の形態5では、実施の形態4と比較し、まず、バージョン選択という工程を別に行なう形態である。以上のように構成しても実施の形態4と同様の効果を得ることができる。そして、実施の形態1の効果に加え、セキュリティ上問題があるアルゴリズムを排除することもできる。

【0106】

以上のように、上記実施の形態における認証方法は、複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する被認証装置から記憶された複数のアルゴリズム識別子と複数の暗号鍵識別子とを認証装置に送信する第1の送信工程と、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する認証装置が、上記第1の送信工程により被認証装置から送信された複数のアルゴリズム識別子と複数の暗号鍵識別子とを受信する第1の受信工程と、上記第1の受信工程により受信された複数のアルゴリズム識別



子と複数の暗号鍵識別子との中に上記認証装置により記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とが存在する場合に、上記認証装置が上記受信工程により受信された複数のアルゴリズム識別子と複数の暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第2の送信工程と、上記被認証装置が上記認証装置から上記第2の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第2の受信工程と、上記第2の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えている。

#### 【0107】

或いは、少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを記憶する被認証装置から記憶された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを認証装置に送信する第1の送信工程と、複数のアルゴリズム識別子と複数の暗号鍵識別子とを記憶する認証装置が、上記第1の送信工程により被認証装置から送信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子とを受信する第1の受信工程と、上記第1の受信工程により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中に上記認証装置により記憶された複数のアルゴリズム識別子の少なくとも1つと複数の暗号鍵識別子の少なくとも1つとが存在する場合に、上記認証装置が上記受信工程により受信された少なくとも1つのアルゴリズム識別子と少なくとも1つの暗号鍵識別子との中から上記認証装置により記憶される所定のアルゴリズム識別子と所定の暗号鍵識別子とを選択する選択工程と、上記選択工程により選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを上記認証装置から上記被認証装置に送信する第2の送信工程と、上記被認証装置が上記認証装置から上記第2の送信工程により送信された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する第2の受信工程と、上記第2の受信工程により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子とに基づいて上記認証装置と上記被認証装置との間で認証処理をおこなう認証処理工程とを備えている。

#### 【0108】

以上の説明において、各実施の形態の説明において「～部」として説明したものは、一部或いはすべてコンピュータで動作可能なプログラムにより構成することができる。これらのプログラムは、例えば、C言語により作成することができる。或いは、HTMLやSGMLやXMLを用いても構わない。

#### 【0109】

図14は、ハードウェア構成図である。

#### 【0110】

以上の説明において、各実施の形態の説明において「～部」として説明したものを、一部或いはすべてコンピュータで動作可能なプログラムにより構成する場合、図14に示すように、通信装置100、200は、プログラムを実行するCPU(Central Processing Unit)37を備えている。CPU37は、内蔵された、或いはバス38を介してRAM(Random Access Memory)40(記憶装置、記憶部の一例である)、外部と通信可能な通信ポート44に接続されている。また、図14に示すように、ROM(Read Only Memory)39、磁気ディスク装置46等の記憶装置に接続されていても構わない。

#### 【0111】

プログラムにより構成する場合、図14におけるプログラム群49には、各実施の形態の説明において「～部」として説明したものにより実行されるプログラムが記憶されている。プログラム群49は、上記記憶装置に記憶されている。プログラム群49は、CPU37、OS47等により実行される。記憶装置は、各処理の結果を記憶する。

#### 【0112】

また、各実施の形態の説明において「～部」として説明したものは、ROM39に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェア或いは、ハードウェア或いは、ソフトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

#### 【0113】

また、上記各実施の形態を実施させるプログラムは、FD (Flexible Disk)、光ディスク、CD (コンパクトディスク)、MD (ミニディスク)、DVD (Digital Versatile Disk) 等のその他の記録媒体による記録装置を用いて記憶されても構わない。係る場合には、図14に示すように、FDD (Flexible Disk Drive) 45、コンパクトディスク装置 (CDD) 86等を備える。

#### 【産業上の利用可能性】

#### 【0114】

このような通信装置100、200は、ETC、ドライブスルー等における店舗側の路側機と自動車側の車載機に限らず、携帯電話等の移動体通信装置間、有線の通信装置間、或いは基地局を経由した有線と無線の通信装置間等における認証装置、被認証装置として、使用することができる。

#### 【図面の簡単な説明】

#### 【0115】

【図1】実施の形態1における認証システムの構成を示す図である。

【図2】実施の形態1における認証方法を示すフローチャート図である。

【図3】通信情報1のフレームの一例を示す図である。

【図4】通信情報2のフレームの一例を示す図である。

【図5】通信情報3のフレームの一例を示す図である。

【図6】通信情報4のフレームの一例を示す図である。

【図7】通信装置200側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムと個別鍵とを示す図である。

【図8】通信装置100側に搭載されているアルゴリズム識別子と暗号鍵識別子とアルゴリズムとを示す図である。

【図9】実施の形態2における認証システムの構成を示す図である。

【図10】実施の形態2における認証方法を示すフローチャート図である。

【図11】実施の形態3における認証方法を示すフローチャート図である。

【図12】実施の形態4における認証方法を示すフローチャート図である。

【図13】実施の形態5における認証方法を示すフローチャート図である。

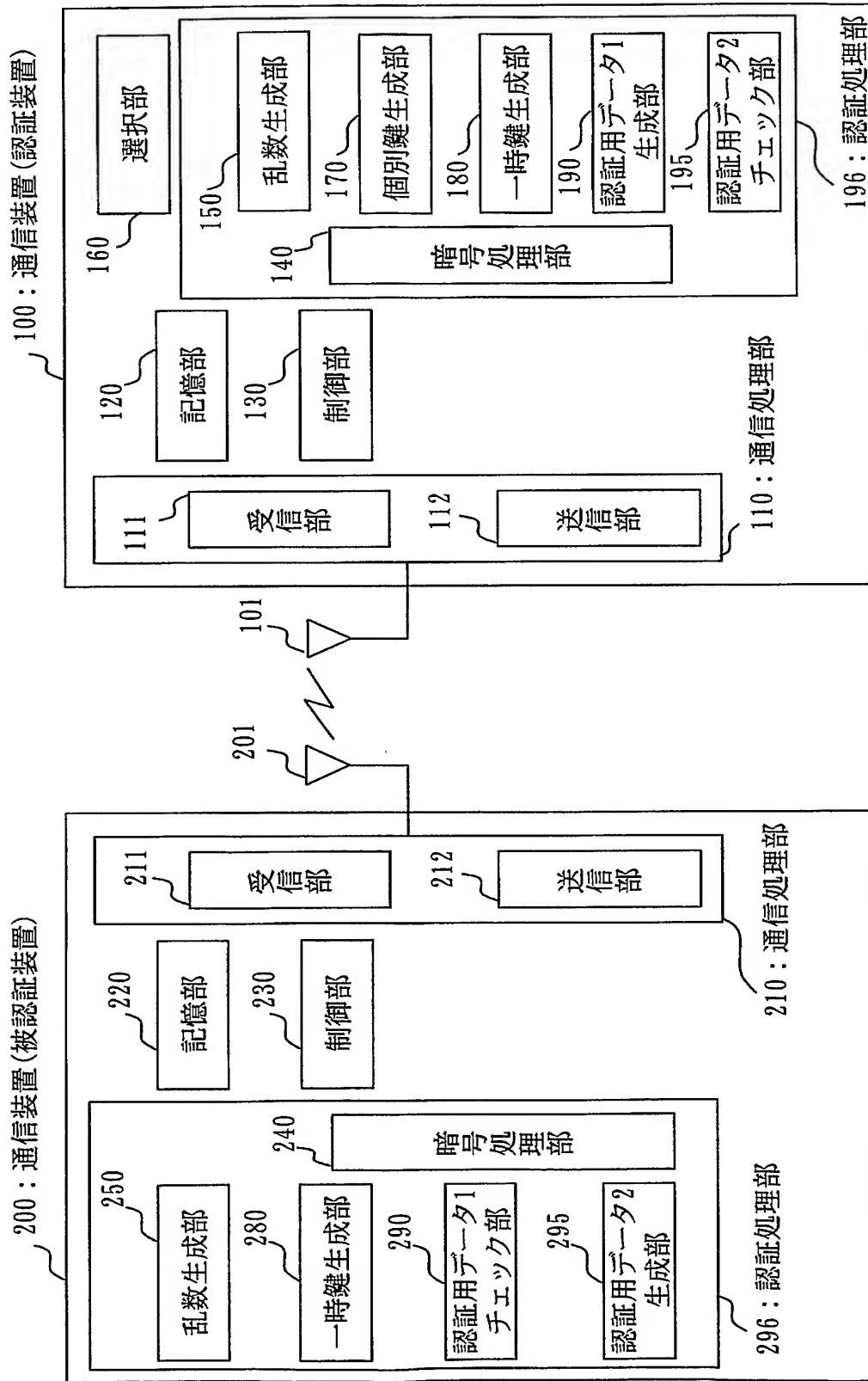
【図14】ハードウェア構成図である。

#### 【符号の説明】

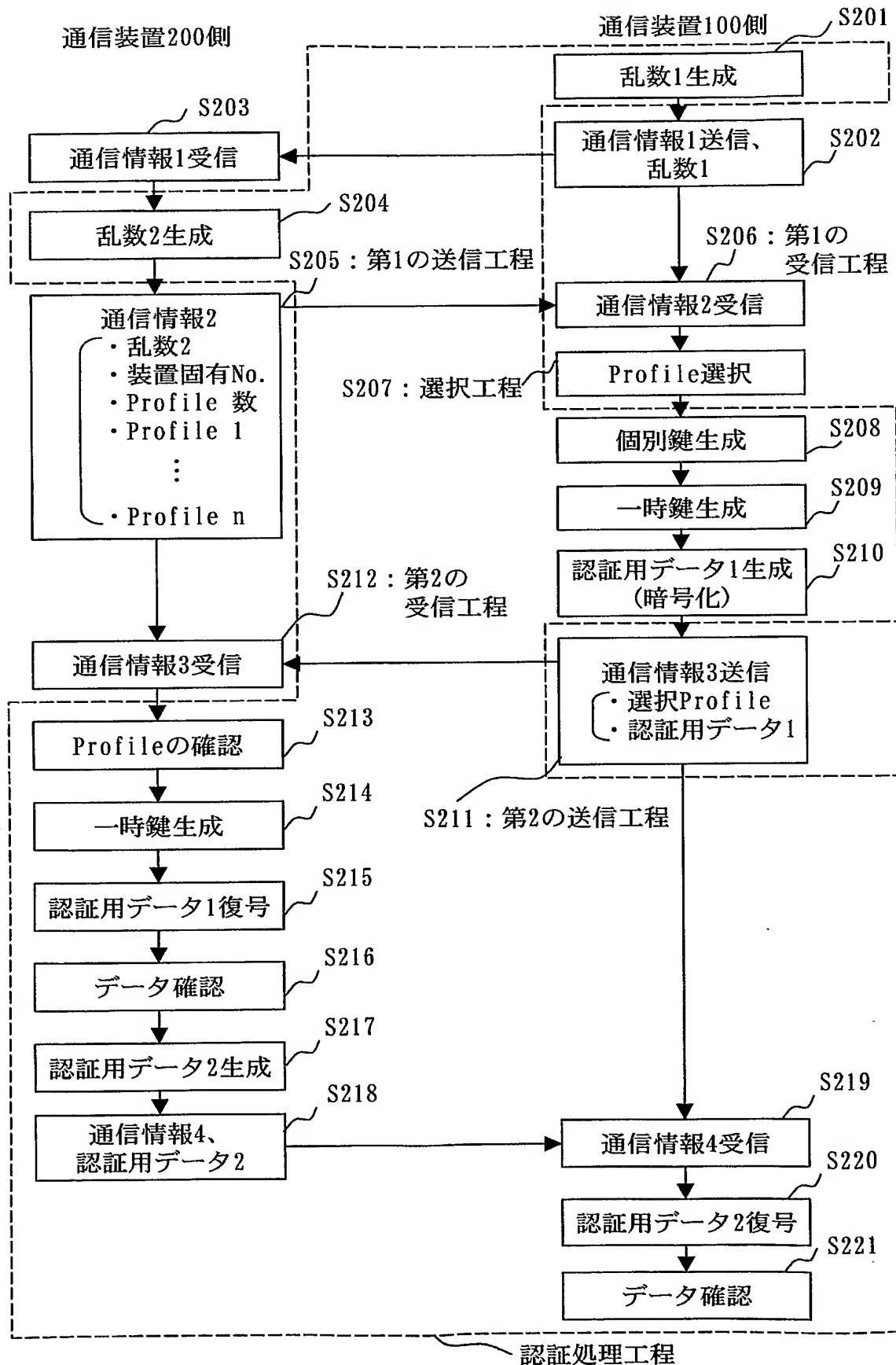
#### 【0116】

37 CPU、38 バス、39 ROM、40 RAM、44 通信ポート、45 FDD、46 磁気ディスク装置、47 OS、49 プログラム群、86 CDD、100 通信装置、101 アンテナ、110 通信処理部、111 受信部、112 送信部、120 記憶部、130 制御部、140 暗号処理部、150 乱数生成部、160 選択部、170 個別鍵生成部、180 一時鍵生成部、190 認証用データ1生成部、195 認証用データ2チェック部、196 認証処理部、200 通信装置、201 アンテナ、210 通信処理部、211 受信部、212 送信部、220 記憶部、230 制御部、240 暗号処理部、250 乱数生成部、280 一時鍵生成部、290 認証用データ1チェック部、291 認証用データ1生成部、295 認証用データ2生成部、296 認証処理部。

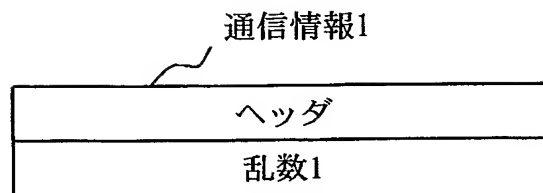
【書類名】 図面  
【図 1】



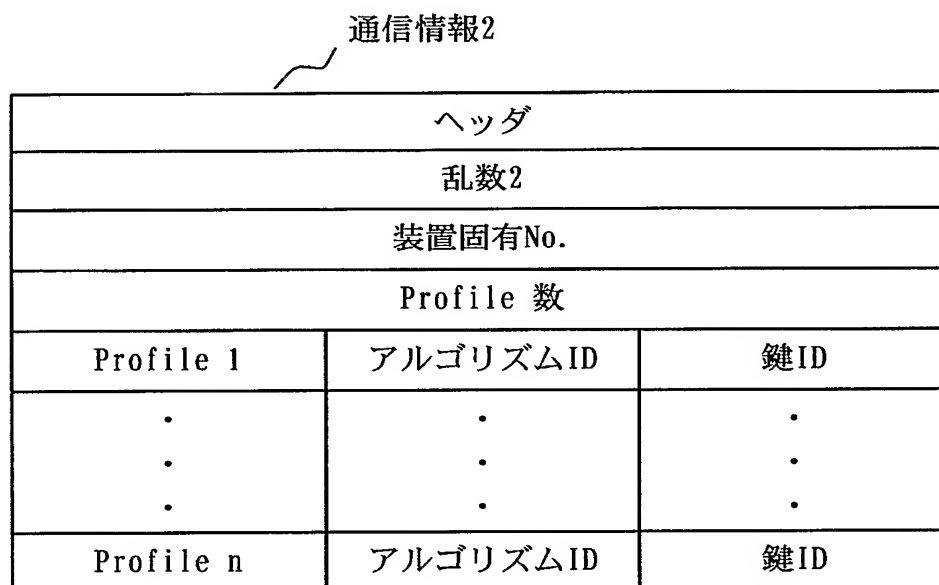
【図 2】



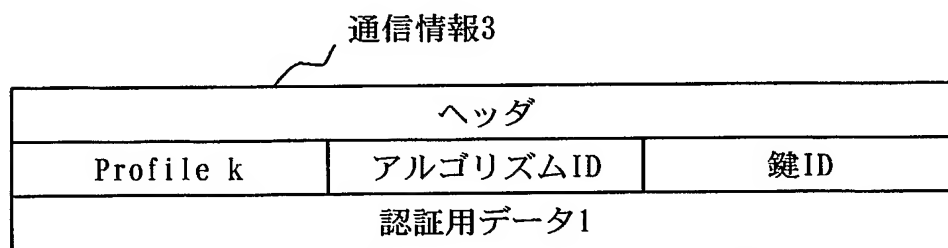
【図 3】



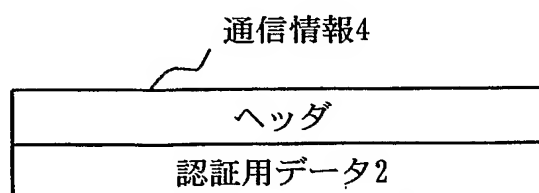
【図 4】



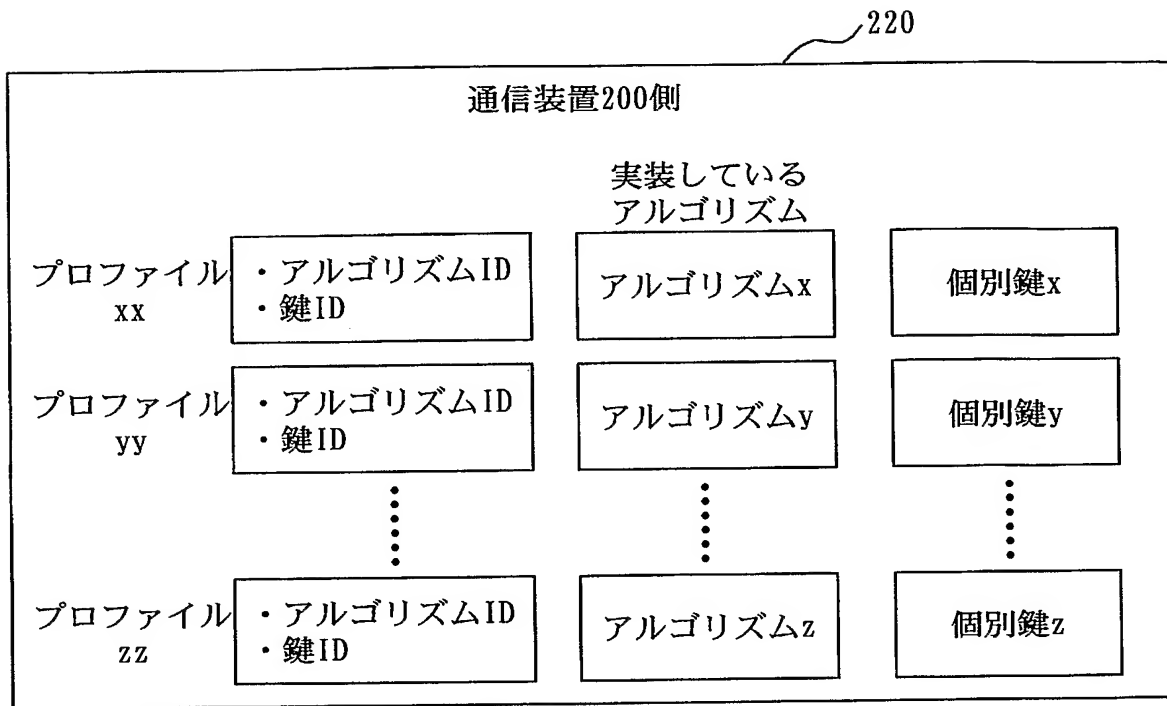
【図 5】



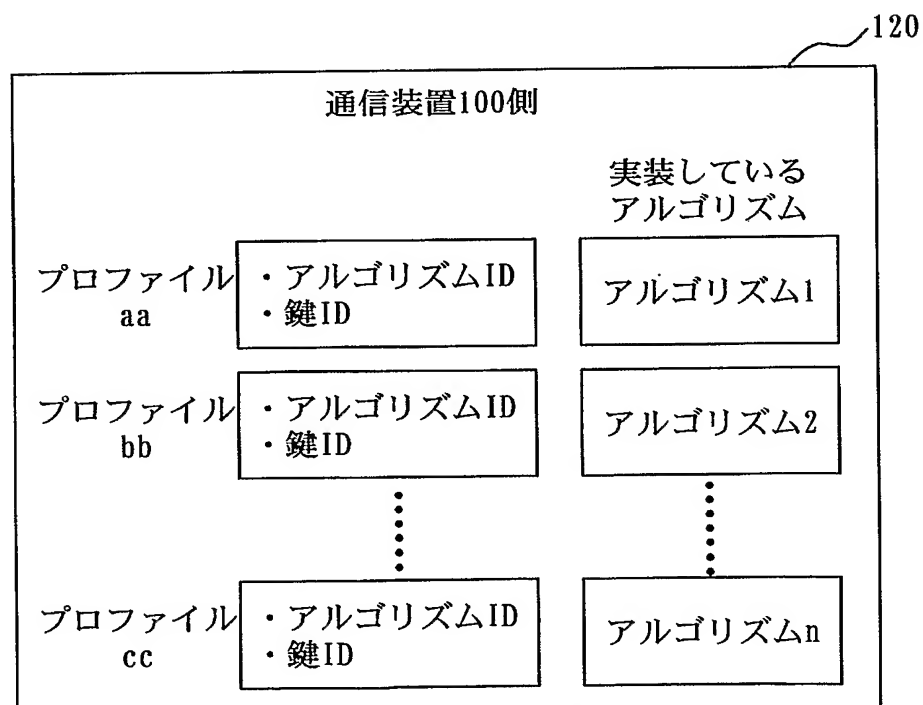
【図 6】



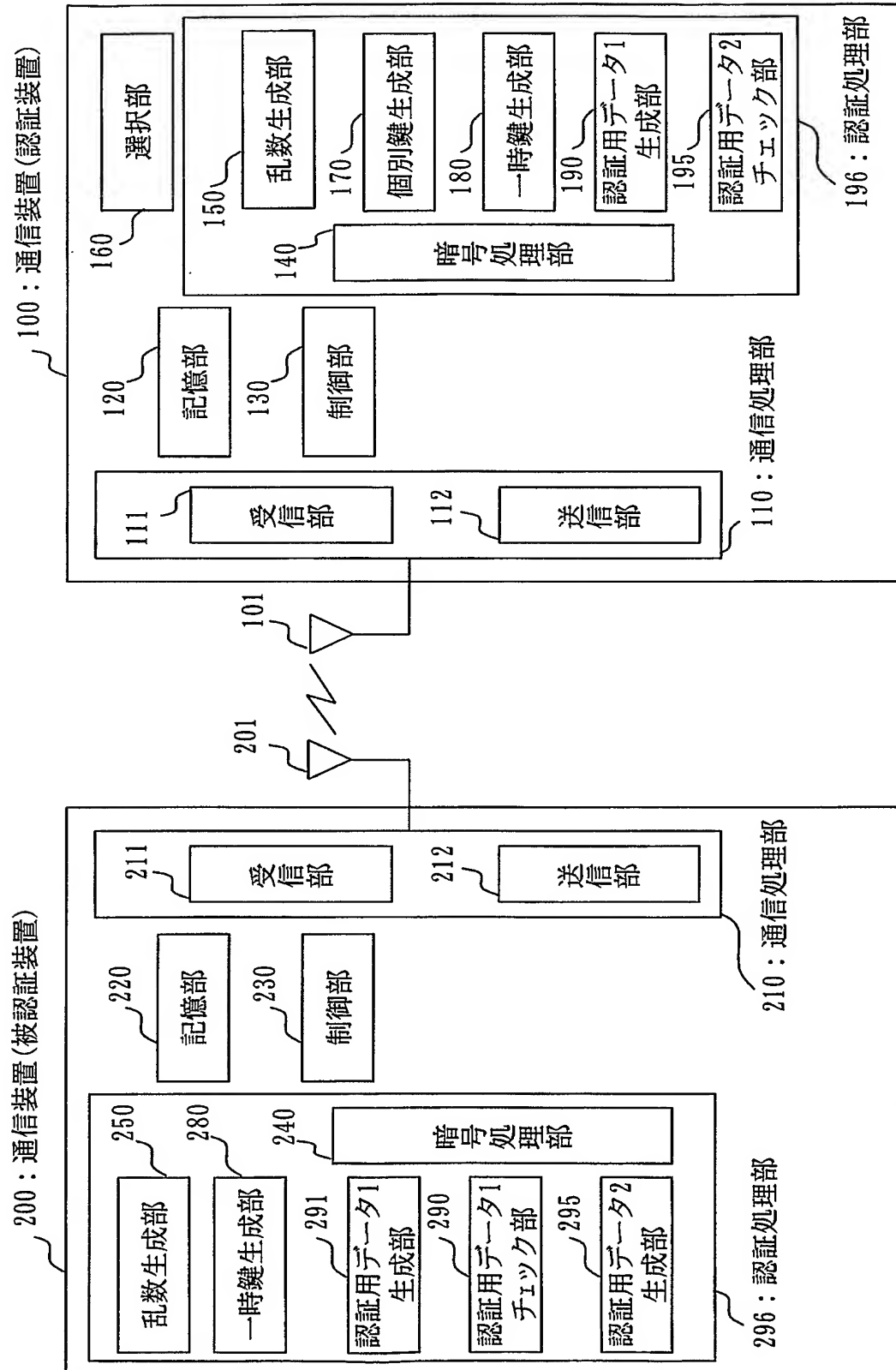
【図 7】



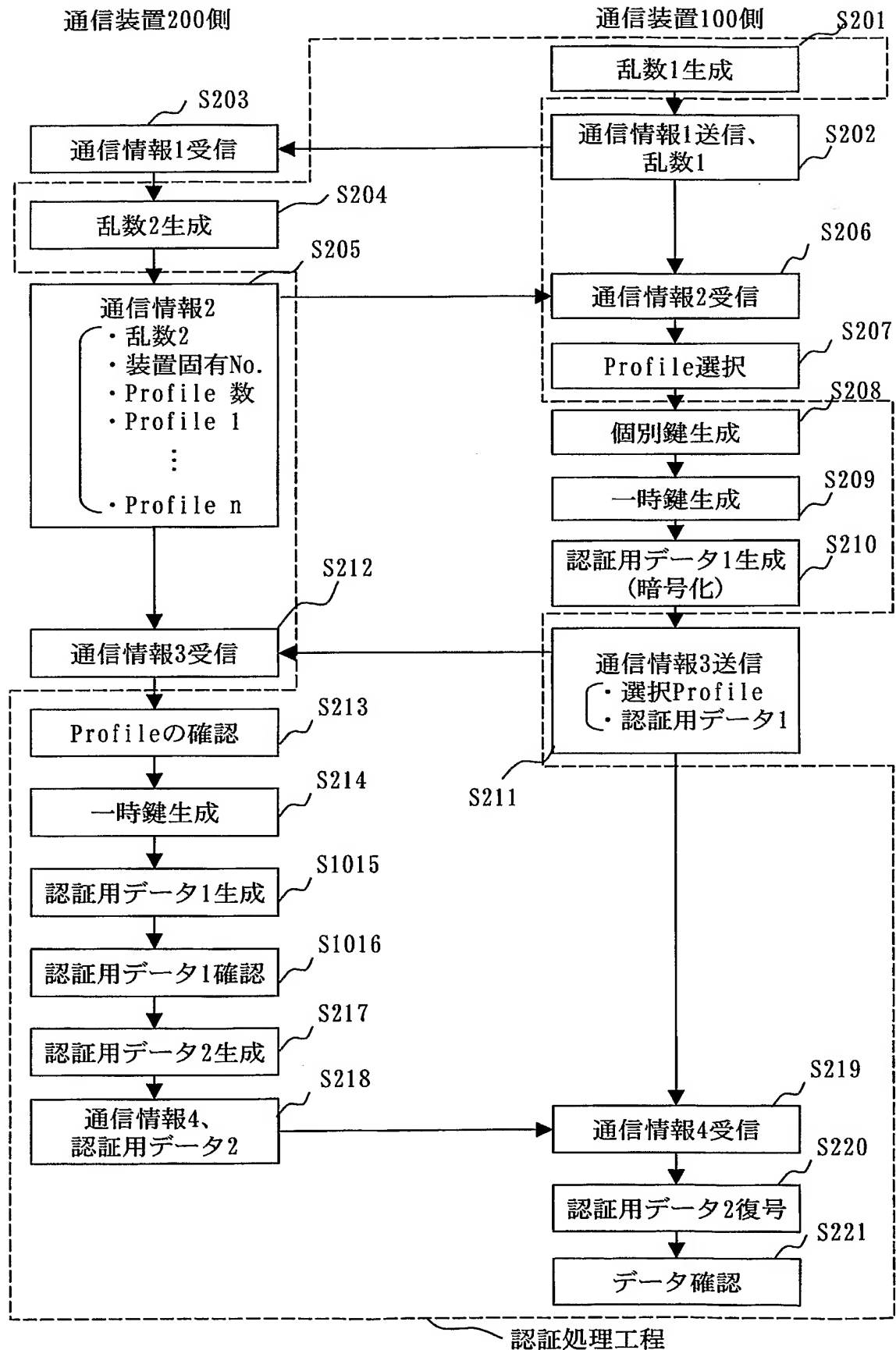
【図 8】



【図 9】

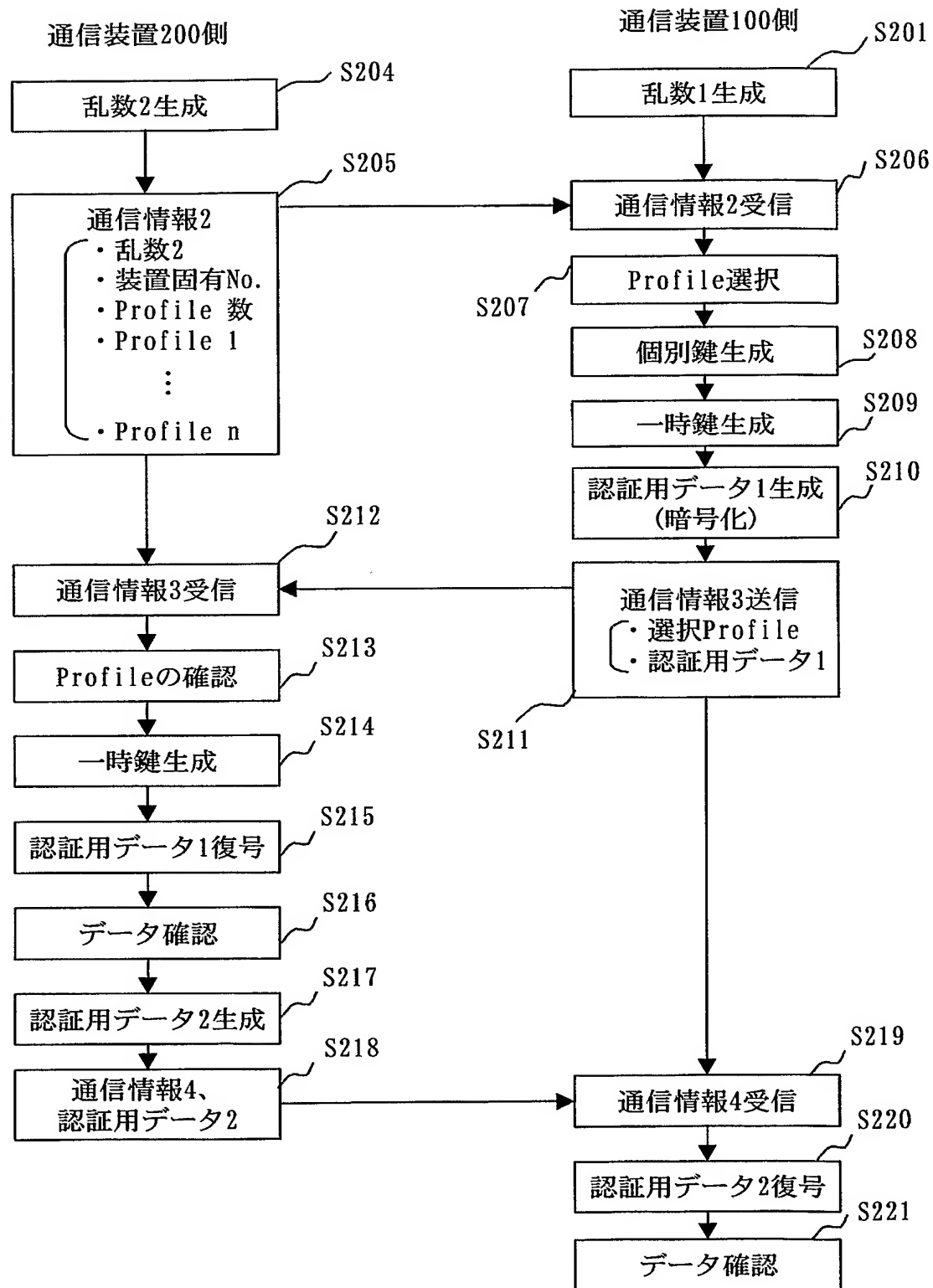


【図 10】

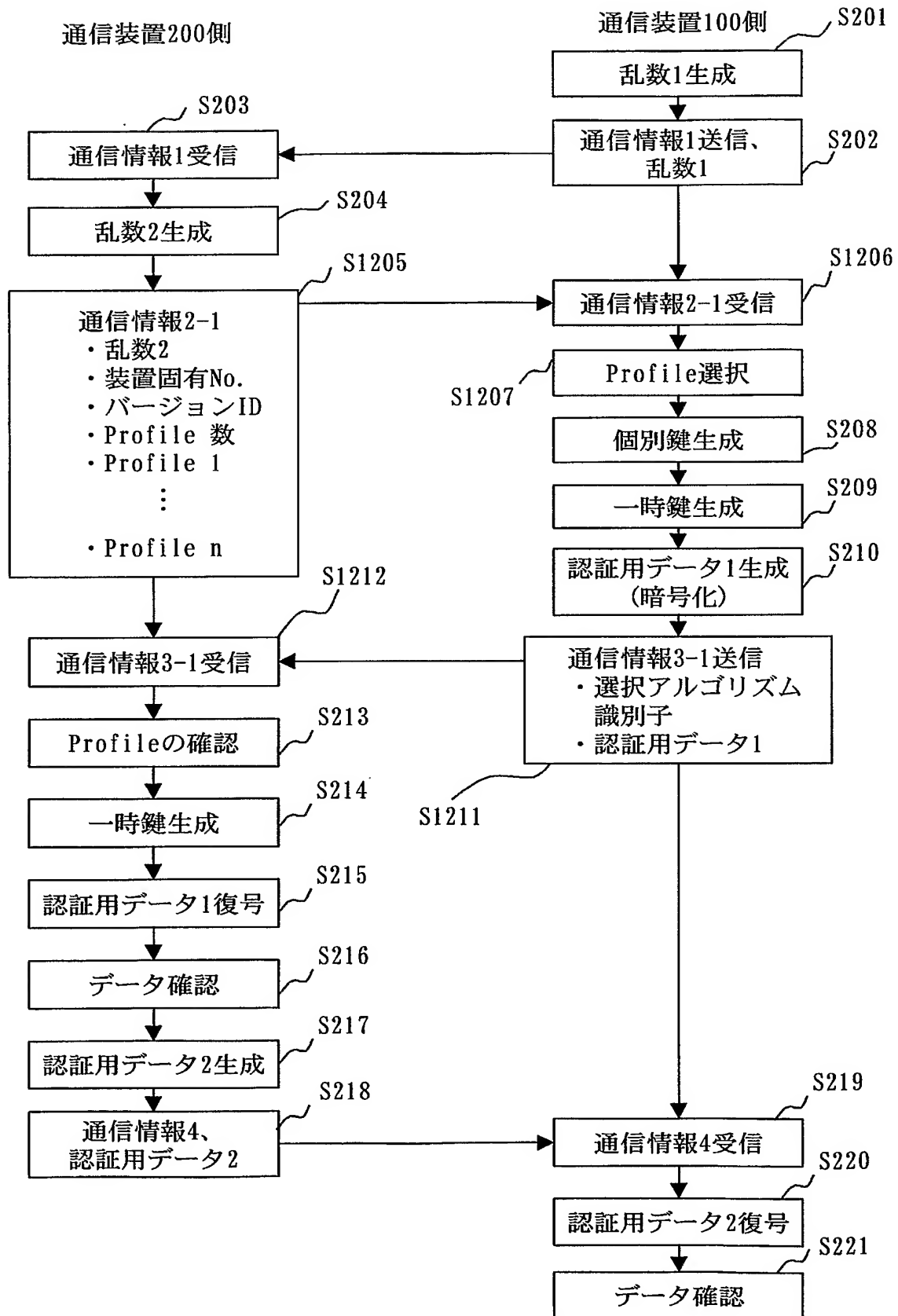




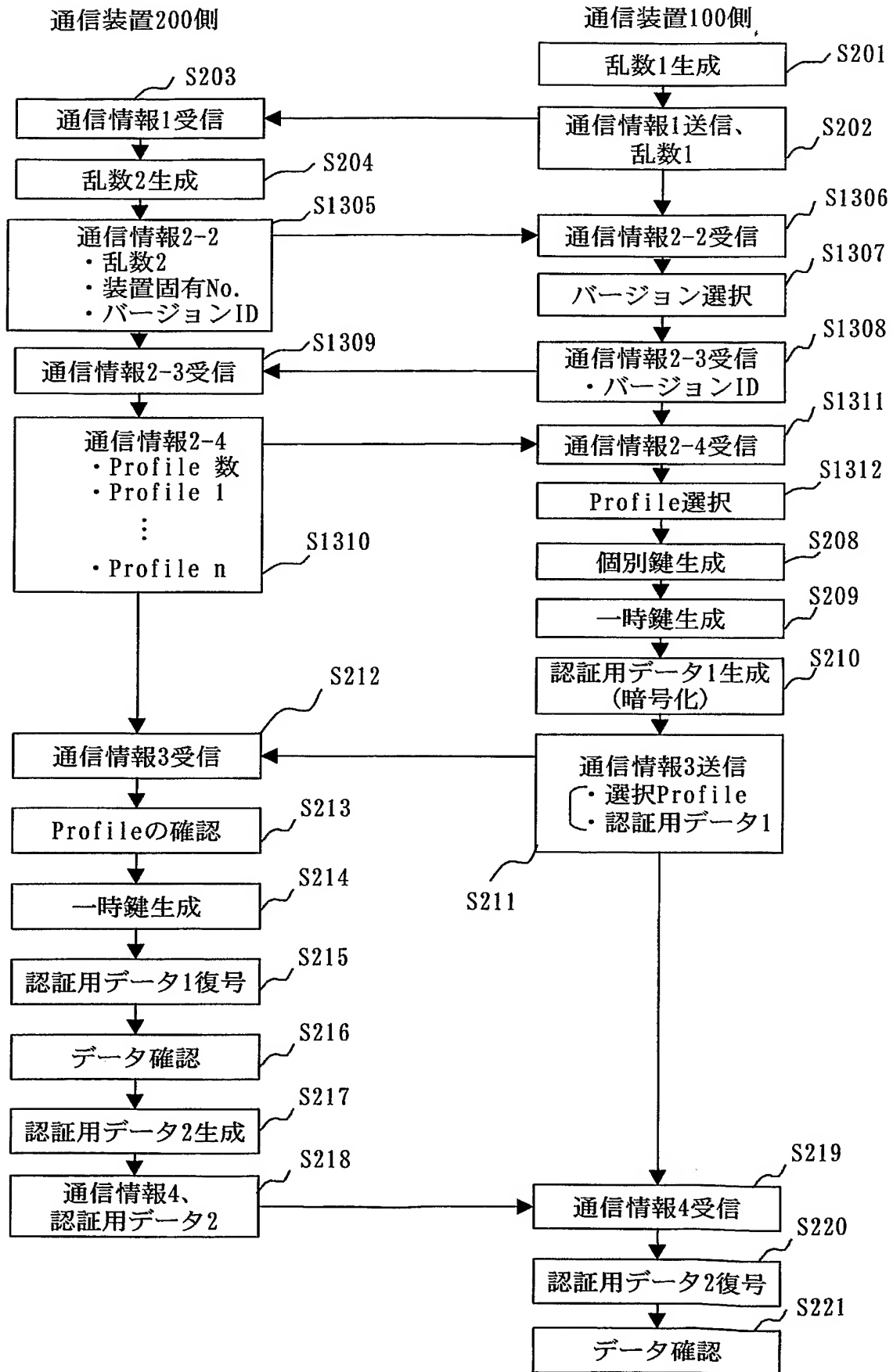
【図 11】



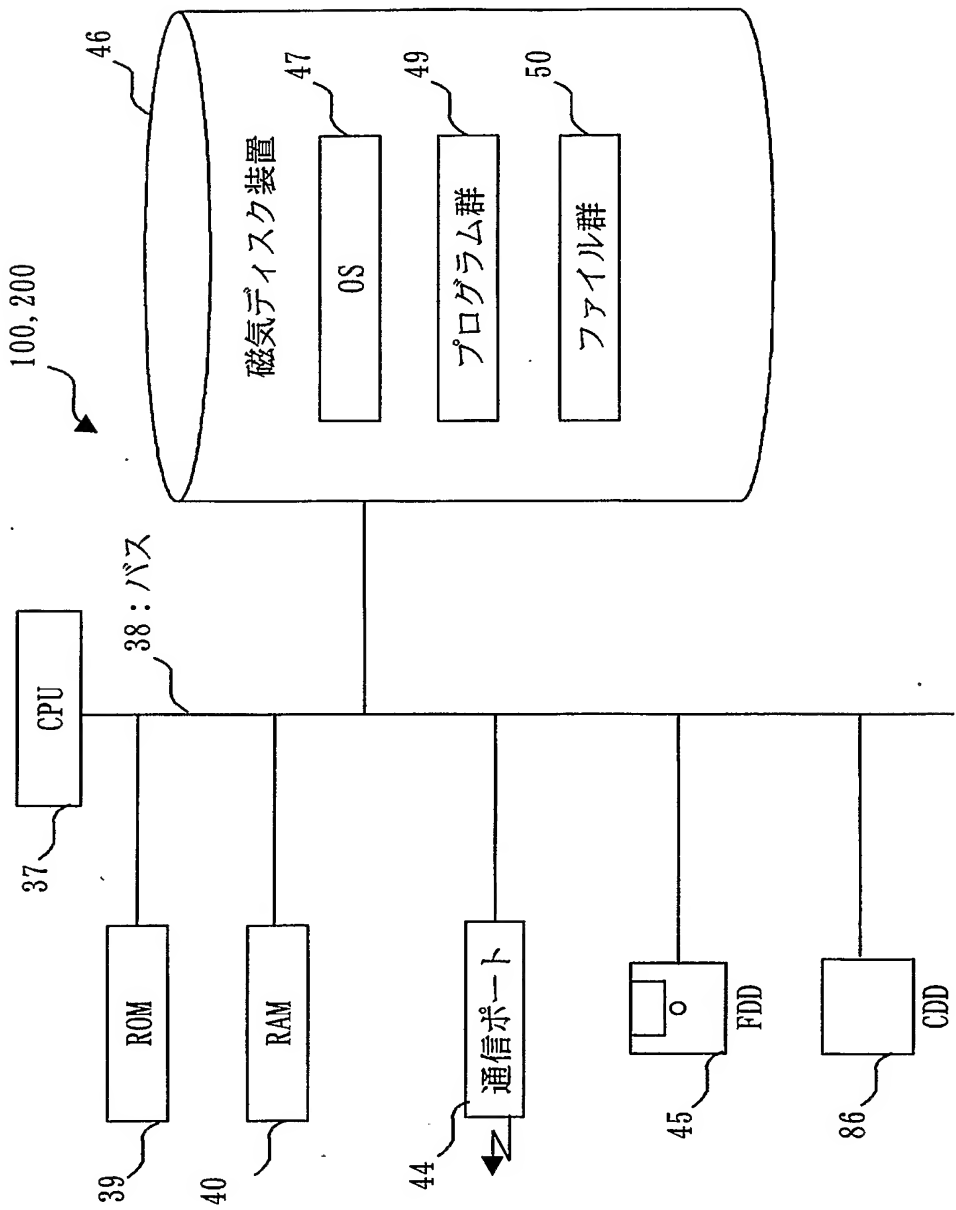
【図 12】




【図 13】



【図 14】





【書類名】 要約書

【要約】

【課題】 搭載しているアルゴリズムが異なるために認証が行なえないといった問題を解決することを目的とする。

【解決手段】 少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを記憶する記憶部 2 2 0 と、上記記憶部 2 2 0 により記憶された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子とを認証装置 1 0 0 に送信する送信部 2 1 2 と、上記認証装置 1 0 0 から上記送信部 2 1 2 により送信された少なくとも 1 つのアルゴリズム識別子と少なくとも 1 つの暗号鍵識別子との中から選択された所定のアルゴリズム識別子と所定の暗号鍵識別子とを受信する受信部 2 1 1 と、上記受信部 2 1 1 により受信された所定のアルゴリズム識別子と所定の暗号鍵識別子に基づいて上記認証装置 1 0 0 との間で認証処理をおこなう認証処理部 2 9 6 とを備えたことを特徴とする。

【選択図】 図 1

特願 2 0 0 3 - 4 3 2 4 7 6

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 6 0 1 3 ]

1. 変更年月日

1 9 9 0 年 8 月 2 4 日

[変更理由]

新規登録

住 所

東京都千代田区丸の内 2 丁目 2 番 3 号

氏 名

三菱電機株式会社